

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-099676

(43)Date of publication of application : 04.04.2003

(51)Int.Cl.

G06F 17/60

G06F 12/14

G09C 1/00

(21)Application number : 2001-288915

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 21.09.2001

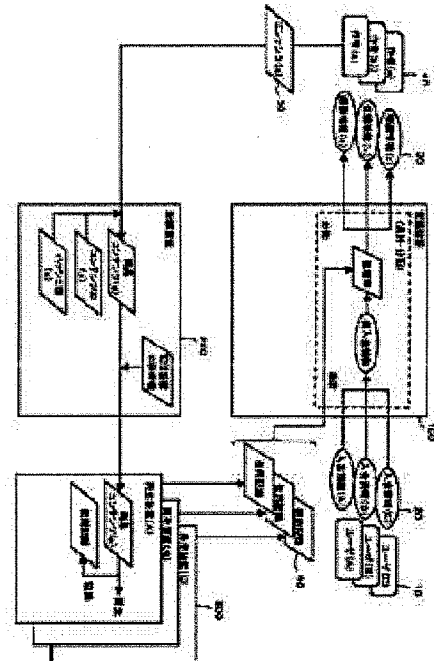
(72)Inventor : FUJII HARUHIKO
SHIONOIRI OSAMU

(54) CONTENT DISTRIBUTION METHOD, CONTENT DISTRIBUTION SYSTEM AND DEVICE FOR THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To ensure free copying and redistribution of contents, dispense with charging process for each delivery of contents and enable peer-to-peer content distribution.

SOLUTION: A delivery device 200 delivers contents to which it adds an encrypted hash value. A reproduction device 200 decodes the encrypted hash value to check the hash value, and if concordance is found, reproduces the contents, holds a use record of each content piece and transmits the use record to a management device 100 at given timing. The management device 100 totalizes receipt information from users to manage total receipts, totalizes the use records to calculate an audience rating of each content piece, and computes a reward to each content author according to the audience rating and the total receipts to distribute it to each author.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-99676

(P2003-99676A)

(43) 公開日 平成15年4月4日 (2003.4.4)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 6 F 17/60	3 3 2	G 0 6 F 17/60	3 3 2 5 B 0 1 7
	3 0 2		3 0 2 E 5 J 1 0 4
12/14	3 1 0	12/14	3 1 0 Z
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 E

審査請求 有 請求項の数14 O L (全 19 頁)

(21) 出願番号 特願2001-288915(P2001-288915)

(22) 出願日 平成13年9月21日 (2001.9.21)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 藤井 治彦

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(72) 発明者 塩野入 理

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(74) 代理人 100073760

弁理士 鈴木 誠

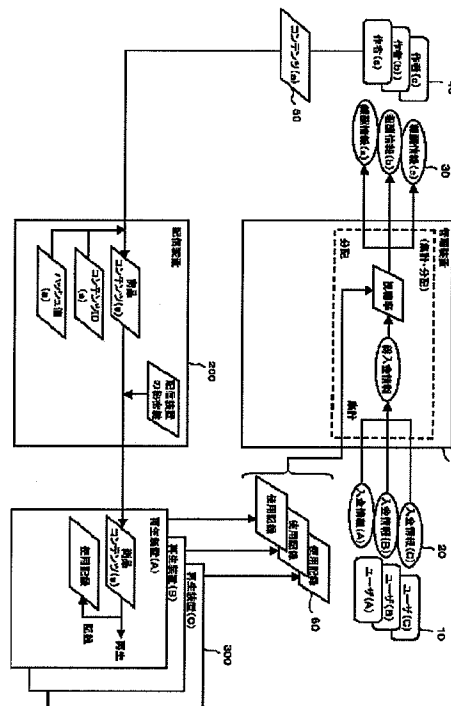
最終頁に続く

(54) 【発明の名称】 コンテンツ流通方法、コンテンツ流通システム及びその装置

(57) 【要約】

【課題】 コンテンツのコピーや再配布が自由で、コンテンツの配信ごとの課金処理を処理を不要とし、また、Peer to Peerでのコンテンツ流通を可能とする。

【解決手段】 配信装置200は、暗号化ハッシュ値を付加してコンテンツを配信する。再生装置200は、暗号化ハッシュ値を復号し、ハッシュ値を照合して、一致した場合、コンテンツを再生するとともに、各コンテンツ別の使用記録を保持して、所定のタイミングで管理装置100に使用記録を送信する。管理装置100は、ユーザからの入金情報を集計して総入金額を管理するとともに、使用記録を集計することにより、各コンテンツ別の視聴率を算出し、該視聴率と総入金額をもとに各コンテンツの作者に対する報酬金額を求め、各作者に分配する。



【特許請求の範囲】

【請求項1】 管理装置、配信装置及び再生装置を有し、配信装置はコンテンツを配信し、再生装置は配信装置の配信したコンテンツを再生するとともに、各コンテンツ別の使用記録を保持し、該保持した使用記録を所定のタイミングで管理装置に送信し、管理装置は再生装置から送付された使用記録を集計して、各コンテンツ別の視聴率を算出するコンテンツ流通方法であって、配信装置は、前記コンテンツを一意に識別するコンテンツIDを生成し、コンテンツのハッシュ値を生成し、前記コンテンツIDとコンテンツのハッシュ値をあわせたデータを暗号化した暗号化情報を生成し、該暗号化情報とコンテンツを組み立てて商品コンテンツとして配信し、再生装置は、配信された商品コンテンツ中の暗号化情報を復号してコンテンツIDとコンテンツのハッシュ値を得るとともに、商品コンテンツ中のコンテンツからそのハッシュ値を生成し、復号して得られたコンテンツのハッシュ値と生成したコンテンツのハッシュ値を比較し、一致していればコンテンツの再生を行い、使用記録を更新する、ことを特徴とするコンテンツ流通方法。

【請求項2】 管理装置、配信装置及び再生装置を有し、配信装置はコンテンツを配信し、再生装置は配信装置の配信したコンテンツを再生するとともに、各コンテンツ別の使用記録を保持し、該保持した使用記録を所定のタイミングで管理装置に送信し、管理装置は再生装置から送付された使用記録を集計して、各コンテンツ別の視聴率を算出するコンテンツ流通方法であって、配信装置は、コンテンツを一意に識別するコンテンツIDを生成し、コンテンツIDとコンテンツをあわせたデータのハッシュ値を生成し、該ハッシュ値を暗号化して暗号化情報を生成し、暗号化情報とコンテンツIDとコンテンツを組み立てて商品コンテンツとして配信し、再生装置は、配信された商品コンテンツ中の暗号化情報を復号化してハッシュ値を得るとともに、商品コンテンツ中のコンテンツIDとコンテンツからハッシュ値を生成し、復号して得られたハッシュ値と生成したハッシュ値を比較し、一致していればコンテンツの再生を行い、使用記録を更新する、ことを特徴とするコンテンツ流通方法。

【請求項3】 管理装置、配信装置及び再生装置を有し、配信装置はコンテンツを配信し、再生装置は配信装置の配信したコンテンツを再生するとともに、各コンテンツ別の使用記録を保持し、該保持した使用記録を所定のタイミングで管理装置に送信し、管理装置は再生装置から送付された使用記録を集計して、各コンテンツ別の視聴率を算出するコンテンツ流通方法であって、配信装置は、コンテンツを一意に識別するコンテンツIDを生成し、コンテンツIDとコンテンツをあわせたデータのハッシュ値を生成し、コンテンツIDとハッシュ

値とコンテンツをあわせたデータを暗号化して商品コンテンツとして配信し、

再生装置は、配信された商品コンテンツを復号化してコンテンツIDとハッシュ値とコンテンツを得、得られたコンテンツIDとコンテンツからハッシュ値を生成し、復号して得られたハッシュ値と生成したハッシュ値を比較し、一致していればコンテンツの再生を行い、使用記録を更新する、ことを特徴とするコンテンツ流通方法。

【請求項4】 請求項1乃至3記載のコンテンツ流通方法において、

管理装置は、ユーザからの入金を集計して総入金額を得、各コンテンツの視聴率と総入金額をもとに各コンテンツの作者等に対する報酬金額を算出して作者等に分配する、ことを特徴とするコンテンツ流通方法。

【請求項5】 請求項4記載のコンテンツ流通方法において、

管理装置は、集計した使用記録をもとに、コンテンツごとに使用回数の和を求め、これに補正値を掛けて、各コンテンツ別の総使用回数を算出し、各コンテンツ別の総使用回数を合計して全コンテンツに対する総使用回数を算出し、各コンテンツの総使用回数を全コンテンツの総使用回数で割ることにより、各コンテンツ別の視聴率を算出する、ことを特徴とするコンテンツ流通方法。

【請求項6】 管理装置、配信装置及び再生装置をネットワークにより接続したコンテンツ流通システムであって、

配信装置は、該配信装置の秘密鍵を保持する手段と、コンテンツを一意に識別するコンテンツIDを生成する手段と、コンテンツのハッシュ値を生成する手段と、コンテンツIDとコンテンツのハッシュ値を秘密鍵で暗号化して暗号化情報を生成する手段と、暗号化情報とコンテンツを組み立てて商品コンテンツを生成して配信する手段を具備し、

再生装置は、配信装置の公開鍵を保持する手段と、配信された商品コンテンツ中の暗号化情報を公開鍵で復号化してコンテンツIDとコンテンツのハッシュ値を得る手段と、商品コンテンツ中のコンテンツからそのハッシュ値を生成する手段と、復号して得られたコンテンツのハッシュ値と生成したコンテンツのハッシュ値を比較する手段と、前記比較の結果、一致していればコンテンツを再生する手段と、各再生コンテンツ別の使用記録を保持する手段と、前記保持された使用記録を所定のタイミングで管理装置へ送信する手段を具備し、

管理装置は、ユーザからの入金を集計して総入金額を保持する手段と、再生装置から送付された使用記録を保持する手段と、前記保持された使用記録を所定のタイミングで集計して、各コンテンツ別の視聴率を算出する手段と、各コンテンツの視聴率と総入金額をもとに各コンテンツの作者等に対する報酬金額を算出し、作者等に分配する手段を具備する、ことを特徴とするコンテンツ流通

システム。

【請求項7】 管理装置、配信装置及び再生装置をネットワークにより接続したコンテンツ流通システムであって、

配信装置は、該配信装置の秘密鍵を保持する手段と、コンテンツを一意に識別するコンテンツIDを生成する手段と、コンテンツIDとコンテンツをあわせたデータのハッシュ値を生成する手段と、該生成したハッシュ値を秘密鍵で暗号化して暗号化情報を生成する手段と、暗号化情報とコンテンツIDとコンテンツを組み立て商品コンテンツを生成して配信する手段を具備し、

再生装置は、配信装置の公開鍵を保持する手段と、配信された商品コンテンツ中の暗号化情報を公開鍵で復号化してハッシュ値を得る手段と、商品コンテンツ中のコンテンツIDとコンテンツからハッシュ値を生成する手段と、復号して得られたハッシュ値と生成したハッシュ値を比較する手段と、前記比較の結果、一致していればコンテンツを再生する手段と、各再生コンテンツ別の使用記録を保持する手段と、前記保持された使用記録を所定のタイミングで管理装置へ送信する手段を具備し、

管理装置は、ユーザからの入金を集計して総入金額を保持する手段と、再生装置から送付された使用記録を保持する手段と、前記保持された使用記録を所定のタイミングで集計して、各コンテンツ別の視聴率を算出する手段と、各コンテンツの視聴率と総入金額をもとに各コンテンツの作者等に対する報酬金額を算出し、作者等に分配する手段を具備する、ことを特徴とするコンテンツ流通システム。

【請求項8】 管理装置、配信装置及び再生装置をネットワークにより接続したコンテンツ流通システムであって、

配信装置は、該配信装置の秘密鍵を保持する手段と、コンテンツを一意に識別するコンテンツIDを生成する手段と、コンテンツIDとコンテンツをあわせたデータのハッシュ値を生成する手段と、コンテンツIDとハッシュ値とコンテンツをあわせたデータを秘密鍵で暗号化して商品コンテンツを生成して配信する手段を具備し、

再生装置は、配信装置の公開鍵を保持する手段と、配信された商品コンテンツを公開鍵で復号化してコンテンツIDとハッシュ値とコンテンツを得る手段と、得られたコンテンツIDとコンテンツからハッシュ値を生成する手段と、復号して得られたハッシュ値と生成したハッシュ値を比較する手段と、前記比較の結果、一致していればコンテンツを再生する手段と、各再生コンテンツ別の使用記録を保持する手段と、前記保持された使用記録を所定のタイミングで管理装置へ送信する手段を具備し、管理装置は、ユーザからの入金を集計して総入金額を保持する手段と、再生装置から送付された使用記録を保持する手段と、前記保持された使用記録を所定のタイミングで集計して、各コンテンツ別の視聴率を算出する手段

と、各コンテンツの視聴率と総入金額をもとに各コンテンツの作者等に対する報酬金額を算出し、作者等に分配する手段を具備する、ことを特徴とするコンテンツ流通システム。

【請求項9】 コンテンツを配信する配信装置であって、該配信装置の秘密鍵を保持する手段と、コンテンツを一意に識別するコンテンツIDを生成する手段と、コンテンツのハッシュ値を生成する手段と、コンテンツIDとコンテンツのハッシュ値を秘密鍵で暗号化して暗号化情報を生成する手段と、暗号化情報とコンテンツを組み立て商品コンテンツを生成して配信する手段を具備することを特徴とする配信装置。

【請求項10】 コンテンツを再生し、使用記録を管理センタへ送付する再生装置であって、コンテンツ配信元の公開鍵を保持する手段と、配信された商品コンテンツ中の暗号化情報を公開鍵で復号化してコンテンツIDとコンテンツのハッシュ値を得る手段と、商品コンテンツ中のコンテンツからそのハッシュ値を生成する手段と、復号して得られたコンテンツのハッシュ値と生成したコンテンツのハッシュ値を比較する手段と、前記比較の結果、一致していればコンテンツを再生する手段と、各再生コンテンツ別の使用記録を保持する手段と、前記保持された使用記録を所定のタイミングで管理装置へ送信する手段を具備することを特徴とする再生装置。

【請求項11】 コンテンツを配信する配信装置であって、該配信装置の秘密鍵を保持する手段と、コンテンツを一意に識別するコンテンツIDを生成する手段と、コンテンツIDとコンテンツをあわせたデータのハッシュ値を生成する手段と、該生成したハッシュ値を秘密鍵で暗号化して暗号化情報を得る手段と、暗号化情報とコンテンツIDとコンテンツを組み立て商品コンテンツを生成して配信する手段を具備することを特徴とする配信装置。

【請求項12】 コンテンツを再生し、使用記録を管理センタへ送付する再生装置であって、コンテンツ配信元の公開鍵を保持する手段と、配信された商品コンテンツ中の暗号化情報を公開鍵で復号化してハッシュ値を得る手段と、商品コンテンツ中のコンテンツIDとコンテンツからハッシュ値を生成する手段と、復号して得られたハッシュ値と生成したコンテンツのハッシュ値を比較する手段と、前記比較の結果、一致していればコンテンツを再生する手段と、各再生コンテンツ別の使用記録を保持する手段と、前記保持された使用記録を所定のタイミングで管理装置へ送信する手段を具備することを特徴とする再生装置。

【請求項13】 コンテンツを配信する配信装置であって、該配信装置の秘密鍵を保持する手段と、コンテンツを一意に識別するコンテンツIDを生成する手段と、コンテンツIDとコンテンツをあわせたデータのハッシュ値を生成する手段と、コンテンツIDとハッシュ値とコ

コンテンツをを合わせたデータを秘密鍵で暗号化して暗号化商品コンテンツを生成して配信する手段を具備することを特徴とする配信装置。

【請求項14】 コンテンツを再生し、使用記録を管理センタへ送付する再生装置であって、コンテンツ配信元の公開鍵を保持する手段と、配信された暗号化商品コンテンツを公開鍵で復号化してコンテンツIDとハッシュ値とコンテンツを得る手段と、得られたコンテンツIDとコンテンツからハッシュ値を生成する手段と、復号して得られたハッシュ値と生成したハッシュ値を比較する手段と、前記比較の結果、一致していればコンテンツを再生する手段と、各再生コンテンツ別の使用記録を保持する手段と、前記保持された使用記録を所定のタイミングで管理装置へ送信する手段を具備することを特徴とする再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、インターネットを介したコンテンツのノンパッケージ流通技術分野に係り、特にコンテンツのコピーや再配布が自由で、コンテンツの配信ごとに課金処理が不要なコンテンツ流通方法及びシステム、その配信装置、再生装置に関する。

【0002】

【従来の技術】従来、コンテンツのノンパッケージ流通方式としては、主に以下の2種類の手法が知られている。

(1) コピープロテクト型

これは、再生装置や記録媒体の固有IDなどを用いてコンテンツを暗号化し、その再生装置や記録媒体以外では再生ができないようにしてから流通させる方式である。この方式では、コンテンツの配信装置にはコピープロテクト処理や課金処理機能が必要となる。

(2) 超流通型

これは、超流通マシン上でしか再生できない超流通コンテンツを作成し、超流通コンテンツはコピー自由とする方式である。ただし、定期的に個人識別情報を含んだ使用記録を管理装置に送信し、ユーザは、この使用記録によって課金される。

【0003】

【発明が解決しようとする課題】上記の従来の手法では、それぞれ以下のような問題点があった。

(1) コピープロテクト型

1. コピープロテクト機能のため、再生装置を交換したり、携帯プレーヤに移して音楽コンテンツを再生することが難しく、利便性が低い。
2. 配信装置にはコピープロテクト処理や課金処理機能が必要なため、汎用のファイル交換ソフトによるPeer to Peerでの流通が難しい。
3. コンテンツの配信ごとに、各配信装置に対してクレジット番号や、どのコンテンツを購入するかといったプ

ライバシー情報を送信する必要がある。

【0004】(2) 超流通型

4. 使用記録によってユーザの課金金額が決まるので、使用記録をユーザの改竄から防御しながら管理装置に安全に定期的に通信する技術が必要である。

5. ユーザの使用記録が課金情報となるので、使用記録には必ず個人を特定する情報が必要であり、誰がどのコンテンツを使用したかという情報が漏洩する可能性があり、プライバシーの問題がある。

10 【0005】このように、従来のコンテンツのノンパッケージ流通では、著作権保護のためにコンテンツにコピープロテクトを課しており、また、ダウンロード毎に課金処理が必要なため利便性やプライバシー面で問題があった。また、Peer to Peerでコンテンツを流通させることにも問題があった。

【0006】本発明の目的は、コンテンツのコピーや再配布が自由で、コンテンツの配信ごとに課金処理を不要とし、また、使用記録の個人を特定する情報も不要である、インターネットを介したコンテンツのノンパッケージ流通を可能にすることにある。

【0007】

【課題を解決するための手段】本発明は、配信装置、再生装置がネットワークを介して接続されたシステムにおいて、配信装置はコンテンツを配信し、再生装置はコンテンツを再生するとともに各コンテンツ別の使用記録を作成し、所定のタイミングで管理装置に使用記録を送信し、管理装置は使用記録を集計することにより、各コンテンツ別の総使用回数と、全コンテンツの総使用回数を求め、各コンテンツの総使用回数の、全コンテンツの総使用回数に対する相対値である視聴率を作成するようにしたものである。

30

【0008】特に、配信装置では、コンテンツを一意に識別するコンテンツIDを生成し、また、コンテンツのハッシュ値を生成し、コンテンツIDとコンテンツのハッシュ値を暗号化した暗号化情報を生成し、該暗号化情報とコンテンツを組み立て商品コンテンツとして配信する。再生装置は、配信された商品コンテンツ中の暗号化情報を復号化してコンテンツIDとコンテンツのハッシュ値を得るとともに、商品コンテンツ中のコンテンツからそのハッシュ値を生成し、復号して得られたコンテンツのハッシュ値と生成したコンテンツのハッシュ値を比較し、一致していればコンテンツの再生を行い、使用記録を更新する。

40

【0009】また、配信装置では、コンテンツIDとコンテンツを合わせたデータのハッシュ値を生成し、該ハッシュ値を暗号化した暗号化情報を生成し、該暗号化情報とコンテンツIDとコンテンツからなる商品コンテンツを配信することでもよい。この場合、再生装置では、商品コンテンツ中の暗号化情報を復号化してハッシュ値を得るとともに、商品コンテンツ中のコンテンツIDと

50

コンテンツからハッシュ値を生成し、復号して得られたハッシュ値と生成したハッシュ値を比較し、一致していればコンテンツの再生を行い、使用記録を更新する。

【0010】また、配信装置では、コンテンツIDとコンテンツをあわせたデータのハッシュ値を生成し、コンテンツIDとハッシュ値とコンテンツをまとめて暗号化し、その暗号化情報を商品コンテンツとして配信することでもよい。この場合、再生装置では、暗号化商品コンテンツを復号化してコンテンツIDとハッシュ値とコンテンツを分離する。その後の処理は、上記の場合と同様である。

【0011】本発明では、全ての再生装置や携帯プレーヤに対してコピーして使用が可能であるため、問題点1は解決する。特に、配信装置の公開鍵をもった再生装置でもってコピーして使用が可能であるため、問題点1は解決する。

【0012】また、本発明では、配信装置にはコピープロテクト処理や課金処理が不要である。暗号化情報の付加されたコンテンツ（商品コンテンツ）は、一切コピープロテクト処理や謝金処理不要で流通できるため、個人のパソコン等からも配信可能である。つまりPeer to Peerでの配信が可能である。よって、問題点2は解決する。

【0013】また、本発明では、配信時に課金処理が不要であるため、クレジットカード番号などのプライバシー情報の送信が不要である。よって、問題点3は解決する。また、本発明では、入金額と使用記録には一切関係がない。すなわち、頻繁にコンテンツをダウンロードして視聴する人も、殆ど視聴しない人も入金額は等しい。よって、ユーザにとって使用記録を改竄するメリットはなく、使用記録の改竄は無くなる。また、多少視聴率が改竄されたとしても視聴率には、ほとんど影響が出ない。よって、問題点4は解決する。

【0014】さらに、本発明では、使用記録は視聴率を算出するためのみに使用されるため、個人を特定する情報は不要である。よって、問題点5は解決する。

【0015】

【発明の実施の形態】以下、図面を参照して本発明の実施例について詳細に説明する。なお、本実施例では、ユーザから強制的かつ定期的に入金があるモデルを想定する。例えば、入金手法として税金を使用することが考えられる。すなわち、全てのユーザ（国民）から入金があるとすると、入金処理の受付は税務署などが行ってもよい。この場合、各個人が入金情報を管理装置に送信する必要はなく、税務署がまとめて管理装置に入金情報の送信を行うようにできる。

【0016】図1は本発明の一実施例によるコンテンツ流通システムの全体的構成図を示す。図1において、100はユーザ（国民）からの入金の管理と各コンテンツの作者等に対する報酬の支払を行う管理装置、200は

作者等からのコンテンツを配信する配信装置、200はコンテンツの再生とその使用記録データを管理装置100へ送信する再生装置である。

【0017】以下に図1の動作概要を説明する。コンテンツの作者等（制作者、発行元など）40は自分のコンテンツ50を配信装置200に送付する。送付の方法は、ネットワークやその他、どのような方法でもよい。

【0018】配信装置200は、コンテンツに対してコンテンツIDを付加する。このコンテンツIDはコンテンツを一意に識別する情報である。次に、コンテンツのハッシュ値を生成し、さらに、コンテンツIDとコンテンツをあわせたデータについて当該配信装置の秘密鍵で暗号化し、該暗号化情報をコンテンツの先頭部に付加することにより商品コンテンツを生成する。配信装置200は、この商品コンテンツをインターネット上に配信する。配信先は、別の配信装置（サーバ）でもかまわないし、Peer to Peerで直接ユーザに配信しても、また、ユーザからユーザへ再配布してもかまわない。なお、配信装置の秘密鍵に対応する公開鍵は、あらかじめ公開しておく。

【0019】ユーザ10は、上記の任意の配信経路を通して、商品コンテンツを無料で入手し、再生装置300にコピーして再生を行う。再生装置300は、コンテンツ再生時、コンテンツ商品中のコンテンツからハッシュ値を生成して記憶する。次に、配信装置の公開鍵を用いて、商品コンテンツに含まれている暗号化された部分を復号し、コンテンツIDとコンテンツのハッシュ値を取り出す。そして、両ハッシュ値を比較し、一致していれば、コンテンツの再生を行う。一方、公開鍵による復号化が失敗したり、ハッシュ値が一致しなかった場合には、改竄が行われたとして再生を中止する。

【0020】再生装置300は、再生を行うと同時に当該コンテンツの使用記録データを更新する。この使用記録データには、各コンテンツIDに対する再生回数（使用回数）、再生日時などが含まれる。ただし、この使用記録データには個人を特定する情報を含めない。

【0021】再生装置300では、例えば1ヶ月に一度等の所定のタイミングで定期的に使用記録データ60を管理装置100に送信する要求を行う。もし再生装置300がインターネットに接続されているのであれば自動的に送信し、携帯端末の様にインターネットに接続されていない場合は、表示部に使用記録の送信要求メッセージを表示する。ユーザはこのメッセージが現れたら携帯端末をインターネットに接続し、使用記録データを管理装置100に対して送信する。

【0022】管理装置100は、各ユーザ（国民）10からの入金情報20を集計して総入金情報を管理している。該管理装置100は、各再生装置300から集められた使用記録データを集計する。なお、集計においては、特定のコンテンツの使用回数が異常に多いとか、ま

たは再生日時をチェックして再生間隔が異常に短く実際は連続的に再生されているとか、同じIPアドレスから連続的に送信されているなど、不審な使用記録データを無効にしてもよい。残った使用記録をもとに、各コンテンツの視聴率を算出する。これらに各々総入金額をかけて、各コンテンツの作者等に対する報酬情報30を作成する。そして、この報酬情報に応じて、徴収された資金(税金)を各作者40等に分配する。

【0023】なお、図1のシステムにおいて、配信装置200では、コンテンツIDとコンテンツをあわせたデータのハッシュ値を生成し、該ハッシュ値を暗号化し、該暗号化情報とコンテンツIDとコンテンツからなる商品コンテンツを配信することでもよい。この場合、再生装置300では、商品コンテンツ中の暗号化情報を復号化してハッシュ値を得るとともに、商品コンテンツ中のコンテンツIDとコンテンツからハッシュ値を生成し、両ハッシュ値を比較して、一致していればコンテンツの再生を行い、使用記録を更新する。

【0024】また、配信装置200では、コンテンツIDとコンテンツをあわせたデータのハッシュ値を生成し、コンテンツIDとハッシュ値とコンテンツをまとめて暗号化し、その暗号化情報を商品コンテンツとして配信することでもよい。この場合、再生装置300では、商品コンテンツを復号化してコンテンツIDとハッシュ値とコンテンツを分離する。その後の処理は、上記の場合と同様である。

【0025】次に、図1のシステムの各実施形態について管理装置100、配信装置200、再生装置300の構成および動作を詳述する。

【0026】〈実施例1〉これは、配信装置200がコンテンツのハッシュ値を生成し、コンテンツIDと該コンテンツのハッシュ値を暗号化し、該暗号化情報をコンテンツに付加して商品コンテンツとして配信するケースである。

【0027】図2は配信装置200の主要部の構成図である。配信装置200は一種のサーバであり、コンテンツID生成部210、ハッシュ値生成部220、暗号化部230、コンテンツ組立部240、秘密鍵保持部250等で構成される。配信装置200はコンテンツの送受信部や鍵生成部、装置全体の動作を制御する制御部等も具備するが、図2では省略してある。鍵生成は周知の方式でよく、生成した鍵のうち、秘密鍵は秘密鍵保持部250が保持し、公開鍵は公開する。

【0028】図3は配信装置200の処理フローチャートを示している。コンテンツの作者等は自分のコンテンツを配信装置200に送付する。配信装置200は、コンテンツを受信すると(ステップ401)、コンテンツID生成部210にて、該コンテンツを一意に識別するコンテンツIDを生成する(ステップ402)。次に、ハッシュ値生成部220において、コンテンツのハッ

シュ値を生成し(ステップ403)、さらに、暗号化部230において、秘密鍵保持部250に保持されている当該配信装置の秘密鍵を用いて、コンテンツIDとハッシュ値を暗号化して暗号化情報を生成する(ステップ404)。コンテンツ組立部240では、この暗号化情報をコンテンツの先頭部に付加することにより商品コンテンツを組み立て(ステップ405)、インターネット等に配信される(ステップ406)。

【0029】図4は再生装置300の主要部の構成図である。再生装置300はパソコン、携帯端末、デジタルテレビ、その他、通信機能とマルチメディア再生機能等を備えた装置の総称である。再生装置300は、コンテンツ分離部310、復号化部320、ハッシュ値生成部330、比較部340、コンテンツ再生部350、使用記録処理部360、使用記録送信処理部370、使用記録蓄積装置380及び公開鍵保持部390等で構成される。図4においても、装置全体の動作を制御する制御部等は省略してある。ここで、ハッシュ値生成部320のアルゴリズムは、配信装置200におけるハッシュ値生成部220のアルゴリズムと同じであり、ユーザから操作不可能になっている。使用記録蓄積装置380は、各コンテンツIDに対する再生回数、再生日時履歴、等からなる使用記録データを格納している。公開鍵保持部390は、配信装置200が公開した公開鍵を保持する。

【0030】図5は再生装置300のコンテンツ再生時の処理フローチャートを示している。ユーザは任意の手法で商品コンテンツを入手し、再生装置300にコピーして再生を行う。再生装置300は、コンテンツ再生時、コンテンツ分離部310にて商品コンテンツを暗号化情報とコンテンツに分離する(ステップ501)。そして、暗号化情報は、復号化部320にて、公開鍵保持部390の公開鍵を用いて復号して元のコンテンツのハッシュ値とコンテンツIDを得る(ステップ502)。また、分離して得られたコンテンツについては、ハッシュ値生成部330にて、あらためてそのハッシュ値を生成する(ステップ503)。次に、比較部330において、両ハッシュ値を比較し(ステップ504)、比較の結果、不一致の場合には再生を中止して終了する。一致の場合は、コンテンツ再生部350及び使用記録処理部360を起動する。コンテンツ再生部350は、起動を受けてコンテンツを再生する(ステップ505)。一方、使用記録処理部360では、コンテンツIDをキーに使用記録蓄積装置380から該当コンテンツIDに対応する使用記録データを読み出して、再生回数の更新や再生日時の追加などを行い(ステップ506)、使用記録蓄積装置380へ再格納する(ステップ507)。

【0031】この再生装置300では、使用記録送信処理部370が一ヶ月毎等、定期的に使用記録蓄積装置380から各使用記録データ(コンテンツID、再生回数、再生日時履歴等)を読み出して管理装置100へ送

信する。そして、送信が正常に終了すると、使用記録蓄積装置380の使用記録データを初期化する。

【0032】なお、再生装置300では、ユーザが故意に再生装置を長期にわたりオフライン状況等にして、ある一定期間、使用記録データの送信が行われない場合、以降の再生を制御するようにしてもよい。また、後述の管理装置100が、使用記録データの受信を監視し、ある一定期間、使用記録データの受信がなかった場合、接続をまってその旨を再生装置300に通知し、これを受けて、再生装置300が以降の再生を制限するようにしてもよい。

【0033】図6は管理装置100の主要部の構成図である。管理装置100は一種のサーバであり、入金情報集計部110、使用記録受信処理部120、使用記録集計部130、コンテンツ視聴率算出部140、報酬情報処理部150及び使用記録蓄積装置160等で構成される。図6においても、装置全体の動作を制御する制御部等は省略してある。使用記録蓄積装置160は、各コンテンツIDに対する使用記録データを格納している。該管理装置100の使用記録蓄積装置160と再生装置300の使用記録蓄積装置380との相違点は、再生装置300の使用記録蓄積装置380が自分の再生装置に対する使用記録データのみしか格納していないのに対し、管理装置100の使用記録蓄積装置160は、各再生装置300から送信されてくる使用記録データを格納していることである。

【0034】管理装置100では、使用記録受信処理部120が再生装置300から送られてきた使用記録データを受信し、使用記録蓄積装置160に格納する。そして、各使用記録データの格納が正常に終了すると、送信元の再生装置300に正常終了メッセージを送信する。なお、受信した複数の使用記録データのうち、一部が正常に終了し、一部が異常の場合には、その旨のメッセージ（例えば、各コンテンツIDごとの正常／異常終了一覧メッセージ等）を送信するようにする。

【0035】図7は管理装置100のコンテンツ作者等への報酬分配時の処理フローチャートを示している。管理装置100では、入金情報集計部110において、各ユーザ（国民）からの入金情報を集計して総入金情報を取得している。該管理装置100は、例えば半年や一年毎に、使用記録集計部130にて使用記録蓄積装置60に蓄積された使用記録データを読み出して使用回数を集計する（ステップ601）。前述したように、この使用記録データ集計においては、特定のコンテンツの使用回数が異常に多いとか、再生間隔が異常に短い、同じIPアドレスから連続的に送信されてくる等、不審な使用記録データを無効にしてもよい。コンテンツ視聴率算出部140では、残った使用記録データをもとに、次のようにして各コンテンツの視聴率を算出する。まず、コンテンツIDごとに使用回数の和を計算し、これに補正値を

かけるなどして、コンテンツ毎の総使用回数（例えば1年の）を算出する（ステップ602）。補正値は、例えば学術論文（テキスト・画像コンテンツ）のように、再生回数が少なくても社会に対する有用性が高いものには大きな値をつけ、猥褻な動画像コンテンツ等に対して低い値をつけ、国歌など著作権のないコンテンツに対してはゼロを与えるなどする。なお、補正値は使用しないことでもよい。次に、ステップ602で求めた各コンテンツ毎の総使用回数を合計して、全コンテンツに対する総使用回数を算出する（ステップ603）。各コンテンツの総使用回数を、それぞれ全コンテンツの総使用回数で割ることにより、各コンテンツ毎の視聴率が求まる（ステップ604）。次に、報酬情報処理部150において、各コンテンツの視聴率にそれぞれ総入金額を掛けて、各コンテンツの作者等に対する報酬情報を作成し（ステップ605）、この報酬情報に応じて、徴収された資金（税金）を各コンテンツの作者等に分配する（ステップ606）。

【0036】なお、管理装置100では、作者等への報酬分配後、使用記録蓄積装置160の使用記録データを初期化するが、例えば二次使用記録蓄積装置を用意して、初期化に先立ち使用記録蓄積装置160の使用記録データを二次使用記録蓄積装置に保存することでもよい。

【0037】〈実施例2〉これは、配信装置200がコンテンツIDとコンテンツをあわせてハッシュ値を生成し、該ハッシュ値を暗号化し、該暗号化情報とコンテンツIDとコンテンツを組み立て商品コンテンツとして配信するケースである。管理装置100の構成は実施例1と同様であるので省略する。

【0038】図8は配信装置200の主要部の構成図であり、図2と同様に、コンテンツID生成部210、ハッシュ値生成部220、暗号化部230、コンテンツ組立部240、秘密鍵保持部250等で構成される。該配信装置の秘密鍵は秘密鍵保持部250が保持し、公開鍵は公開する。

【0039】図9は配信装置200の処理フローチャートを示している。コンテンツの作者等は自分のコンテンツを配信装置200に送付する。配信装置200は、コンテンツを受信すると（ステップ701）、コンテンツID生成部210にて、該コンテンツを一意に識別するコンテンツIDを生成する（ステップ702）。次に、ハッシュ値生成部220において、コンテンツとコンテンツIDをあわせたデータのハッシュ値を生成し（ステップ703）、さらに、暗号化部230において、秘密鍵保持部250に保持されている当該配信装置の秘密鍵を用いてハッシュ値を暗号化する（ステップ704）。コンテンツ組立部240では、この暗号化されたハッシュ値（暗号化情報）を、コンテンツIDとコンテンツからなるデータの先頭部に付加することにより商品コンテ

ンツを組み立て（ステップ705）、インターネット等に配信される（ステップ706）。

【0040】図10は再生装置300の主要部の構成図であり、図4と同様に、コンテンツ分離部310、復号化部320、ハッシュ値生成部230、比較部340、コンテンツ再生部350、使用記録処理部360、使用記録送信処理部370、使用記録蓄積装置380及び公開鍵保持部390等で構成される。ここでも、ハッシュ値生成部320のアルゴリズムは、配信装置200におけるハッシュ値生成部220のアルゴリズムと同じであり、ユーザから操作不可能になっている。使用記録蓄積装置380は、各コンテンツIDに対する再生回数、再生日時履歴、等からなる使用記録データを格納している。公開鍵保持部390は、配信装置200が公開した公開鍵を保持する。

【0041】図11は再生装置300のコンテンツ再生時の処理フローチャートを示している。ユーザは任意の手法で商品コンテンツを入手し、再生装置300にコピーして再生を行う。再生装置300は、コンテンツ再生時、コンテンツ分離部310にて商品コンテンツを暗号化情報、コンテンツID、コンテンツに分離する（ステップ801）。そして、暗号化情報は、復号化部320にて、公開鍵保持部390の公開鍵を用いて復号して元のハッシュ値を得（ステップ802）、分離して得られたコンテンツIDとコンテンツについては、ハッシュ値生成部330にて、あらためてこれらをあわせたハッシュ値を生成する（ステップ803）。次に、比較部330において、両ハッシュ値を比較し（ステップ804）、比較の結果、不一致の場合には再生を中止して終了する。一致の場合は、コンテンツ再生部350及び使用記録処理部360を起動する。コンテンツ再生部350は、起動を受けてコンテンツを再生する（ステップ805）。一方、使用記録処理部360では、コンテンツIDをキーに使用記録蓄積装置380から該当コンテンツIDに対応する使用記録データを読み出して、再生回数の更新や再生日時の追加などを行い（ステップ806）、使用記録蓄積装置380へ再格納する（ステップ807）。

【0042】〈実施例3〉これは、配信装置がコンテンツIDとコンテンツをあわせてハッシュ値を生成し、コンテンツID、該ハッシュ値、コンテンツをまとめて暗号化し、該暗号化情報を商品コンテンツ（暗号化商品コンテンツ）として配信するケースである。管理装置100の構成は実施例1と同様であるので省略する。

【0043】図12は配信装置200の主要部の構成図である。配信装置200はコンテンツID生成部210、ハッシュ値生成部220、秘密鍵保持部250、暗号化部1200等で構成される。該配信装置の秘密鍵は秘密鍵保持部250が保持し、公開鍵は公開する。

【0044】図13は配信装置200の処理フローチャ

ートを示している。コンテンツの作者等は自分のコンテンツを配信装置200に送付する。配信装置200は、コンテンツを受信すると（ステップ901）、コンテンツID生成部210にて、該コンテンツを一意に識別するコンテンツIDを生成する（ステップ902）。次に、ハッシュ値生成部220において、コンテンツとコンテンツIDをあわせたデータのハッシュ値を生成する（ステップ903）、次に、暗号化部1200において、秘密鍵保持部250に保持されている当該配信装置の秘密鍵を用いて、コンテンツIDとハッシュ値とコンテンツをまとめて暗号化し（ステップ904）、暗号化商品コンテンツをインターネット等に配信される（ステップ905）。

【0045】図14は再生装置300の主要部の構成図である。再生装置300は、復号化部1300、ハッシュ値生成部330、比較部340、コンテンツ再生部350、使用記録処理部360、使用記録送信処理部370、使用記録蓄積装置380及び公開鍵保持部390等で構成される。ここで、ハッシュ値生成部320のアルゴリズムは、配信装置200におけるハッシュ値生成部220のアルゴリズムと同じであり、ユーザから操作不可能になっている。使用記録蓄積装置380は、各コンテンツIDに対する再生回数、再生日時履歴、等からなる使用記録データを格納している。公開鍵保持部390は、配信装置200が公開した公開鍵を保持する。

【0046】図15は再生装置300のコンテンツ再生時の処理フローチャートを示している。ユーザは任意の手法で商品コンテンツ（暗号化商品コンテンツ）を入手し、再生装置300にコピーして再生を行う。再生装置300は、コンテンツ再生時、暗号化商品コンテンツを復号してコンテンツID、ハッシュ値、コンテンツを得る（ステップ1001）。次に、得られたコンテンツIDとコンテンツについては、ハッシュ値生成部330にて、あらためてこれらをあわせたハッシュ値を生成する（ステップ1002）。次に、比較部330において、両ハッシュ値を比較し（ステップ1003）、比較の結果、不一致の場合には再生を中止して終了する。一致の場合は、コンテンツ再生部350及び使用記録処理部360を起動する。コンテンツ再生部350は、起動を受けてコンテンツを再生する（ステップ1004）。一方、使用記録処理部360では、コンテンツIDをキーに使用記録蓄積装置380から該当コンテンツIDに対応する使用記録データを読み出して、再生回数の更新や再生日時の追加などを行い（ステップ1005）、使用記録蓄積装置380へ再格納する（ステップ1006）。

【0047】以上、本発明の実施例を説明したが、管理装置、配信装置、再生装置の処理手順は、コンピュータで実行可能なプログラムとして、あらかじめフロッピー（登録商標）ディスク、CD-ROM、その他の記録媒

体に記録して提供することも可能である。

【0048】

【発明の効果】以上説明したように、本発明によれば、インターネットを介したコンテンツ流通システムにおいて、コンテンツのコピーや再配布が自由で、コンテンツの配信ごとの課金処理も不要であり、利便性やプライバシー面で優れ、また、容易にPeer to Peerでコンテンツを流通させることも可能になる。

【図面の簡単な説明】

【図1】本発明の一実施例のシステム構成図である。

【図2】実施例1の配信装置の詳細構成図である。

【図3】図2の配信装置のコンテンツ配信処理フロー図である。

【図4】実施例1の再生装置の詳細構成図である。

【図5】図4の再生装置のコンテンツ再生時の処理フロー図である。

【図6】管理装置の詳細構成図である。

【図7】図6の管理装置の報酬分配時の処理フロー図である。

【図8】実施例2の配信装置の詳細構成図である。

【図9】図8の配信装置のコンテンツ配信処理フロー図

である。

【図10】実施例2の再生装置の詳細構成図である。

【図11】図10の再生装置のコンテンツ再生時の処理フロー図である。

【図12】実施例3の配信装置の詳細構成図である。

【図13】図12の配信装置のコンテンツ配信処理フロー図である。

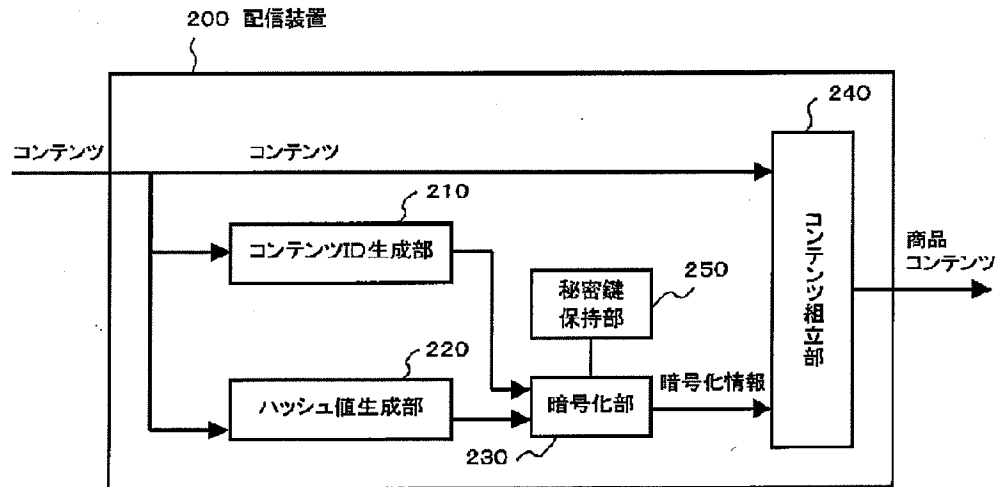
【図14】実施例3の再生装置の詳細構成図である。

【図15】図14の再生装置のコンテンツ再生時の処理フロー図である。

【符号の説明】

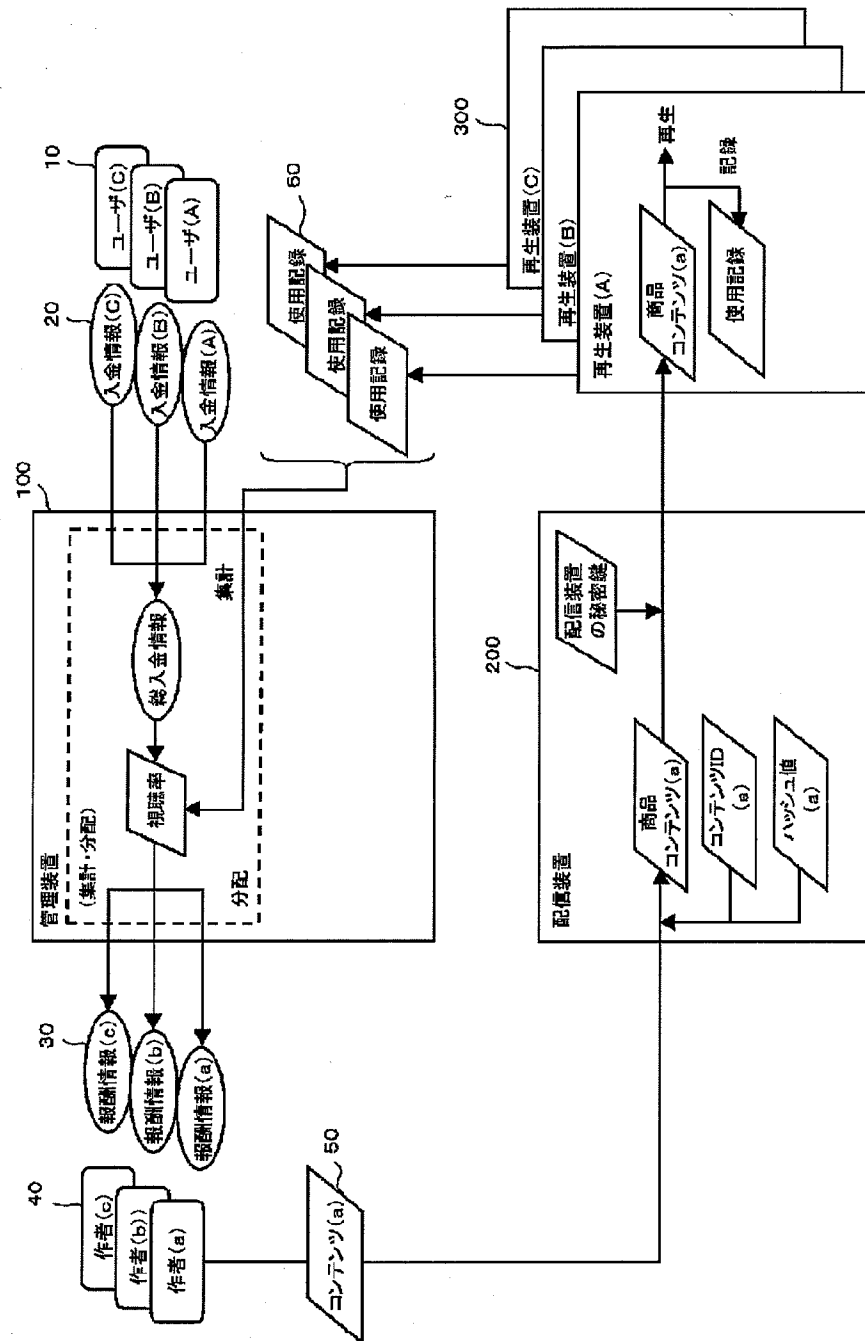
10	ユーザ
20	入金情報
30	報酬情報
40	作者
50	コンテンツ
60	使用記録
100	管理装置
200	配信装置
300	再生装置

【図2】

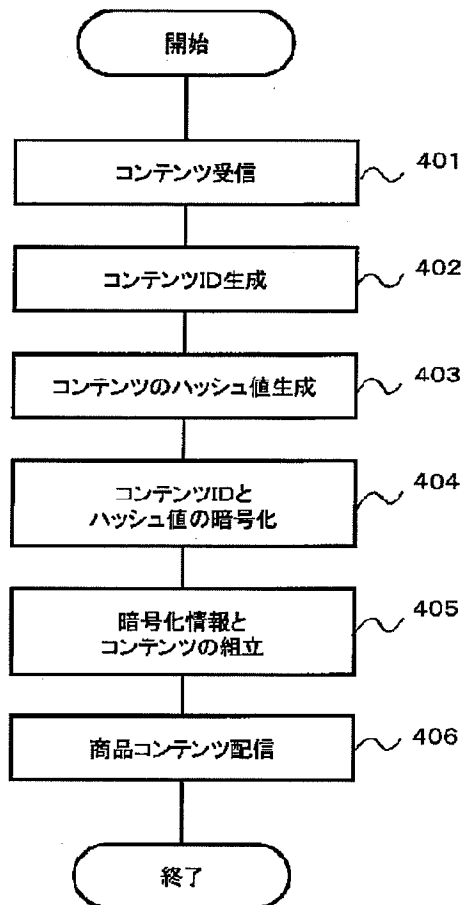


配信装置の構成図

【図1】

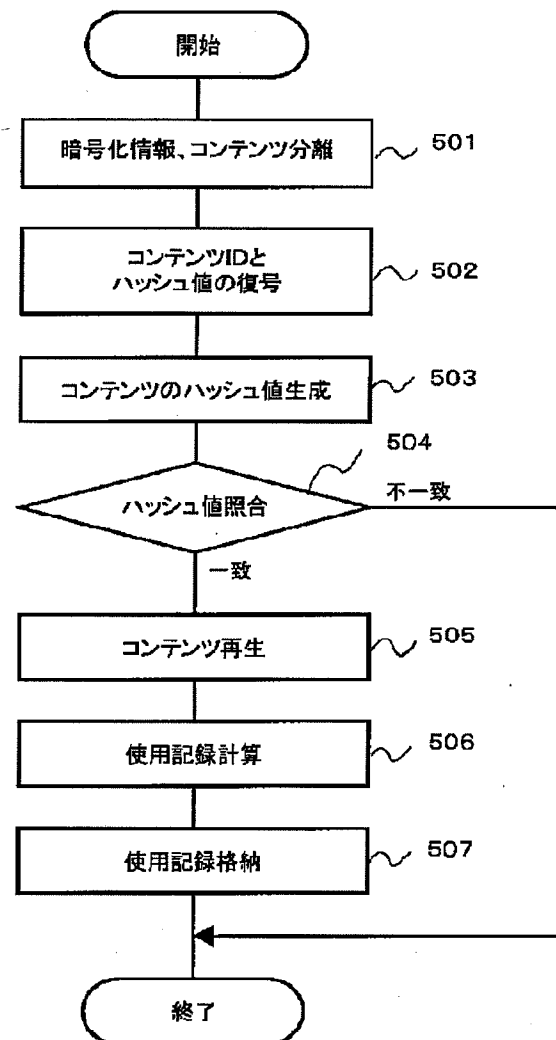


【図3】



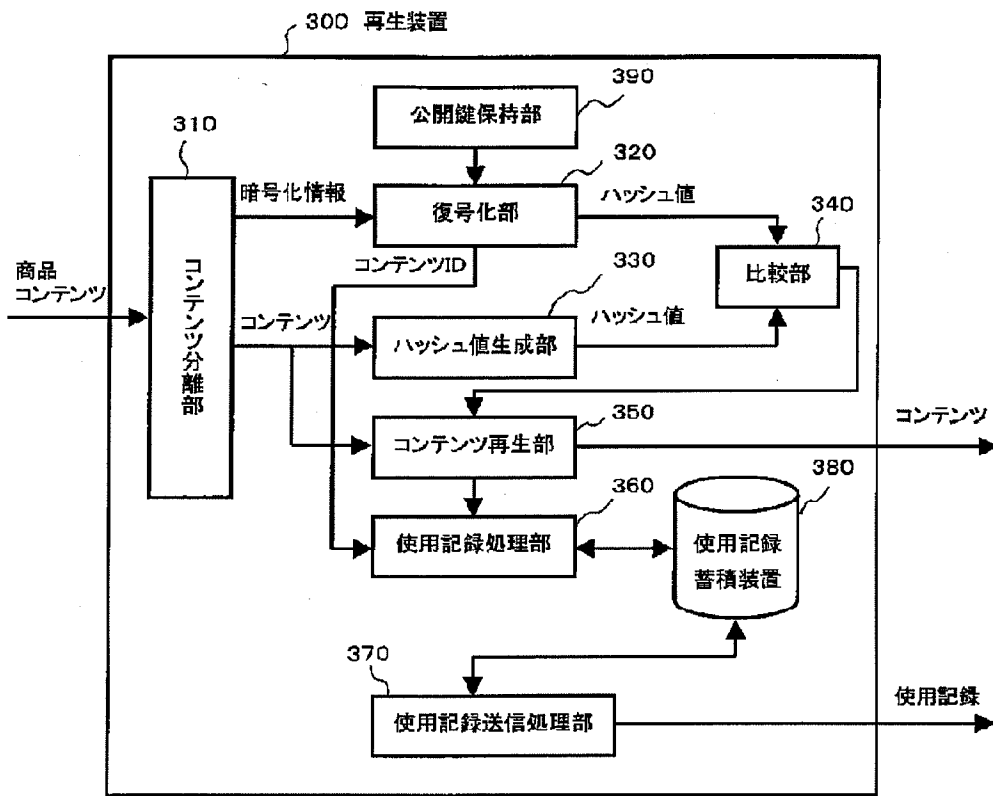
コンテンツ配信処理フロー図

【図5】



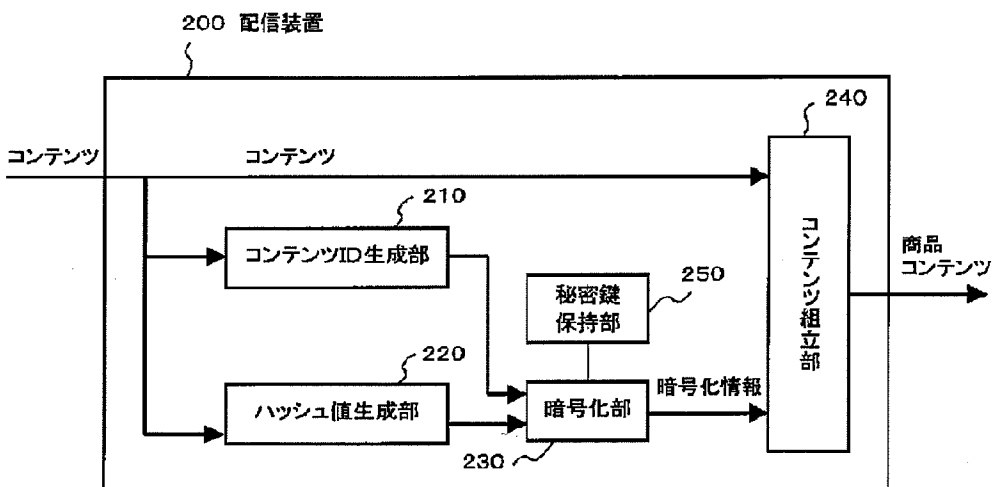
再生時の処理フロー

【図4】



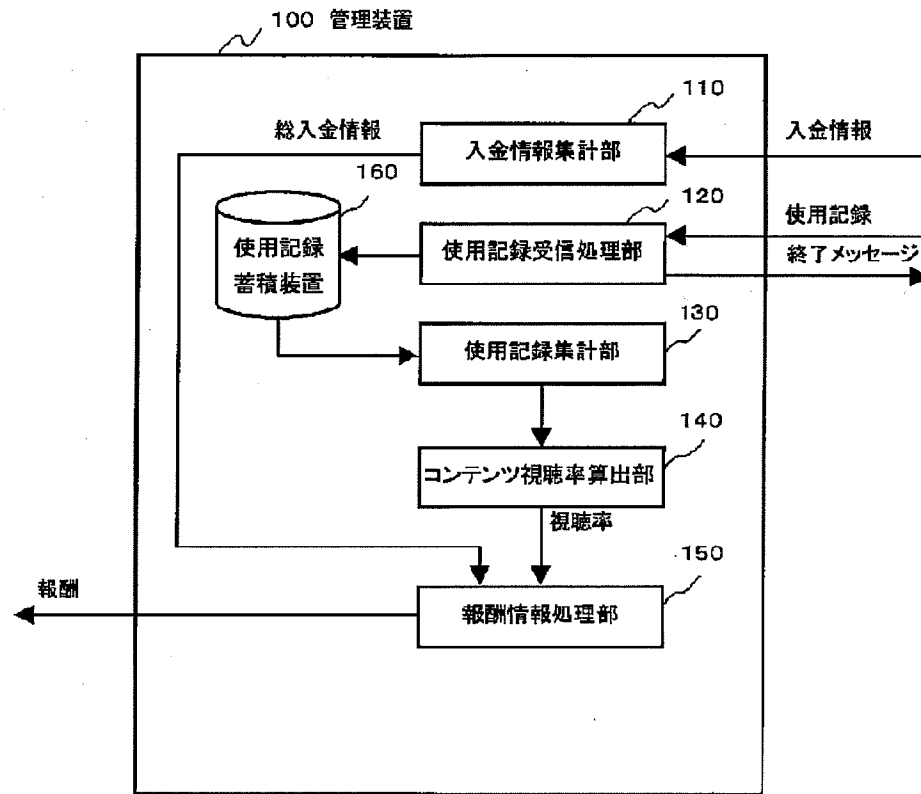
再生装置の構成図

【図8】



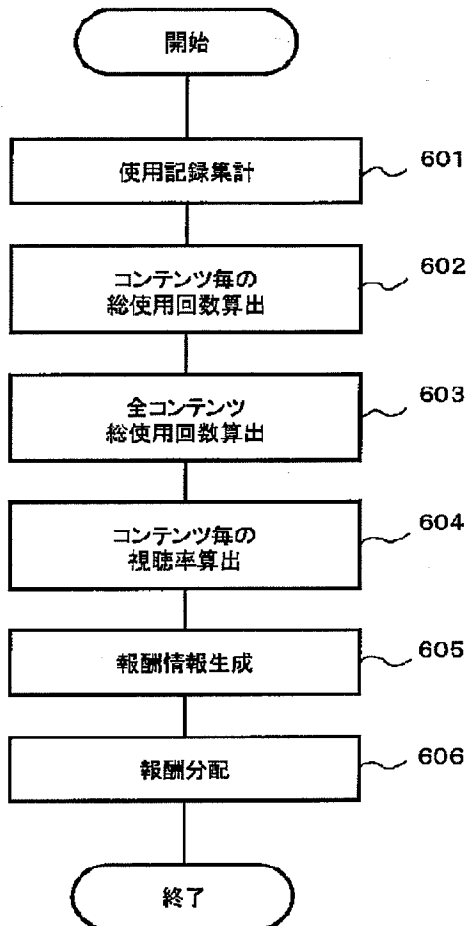
配信装置の構成図

【図6】



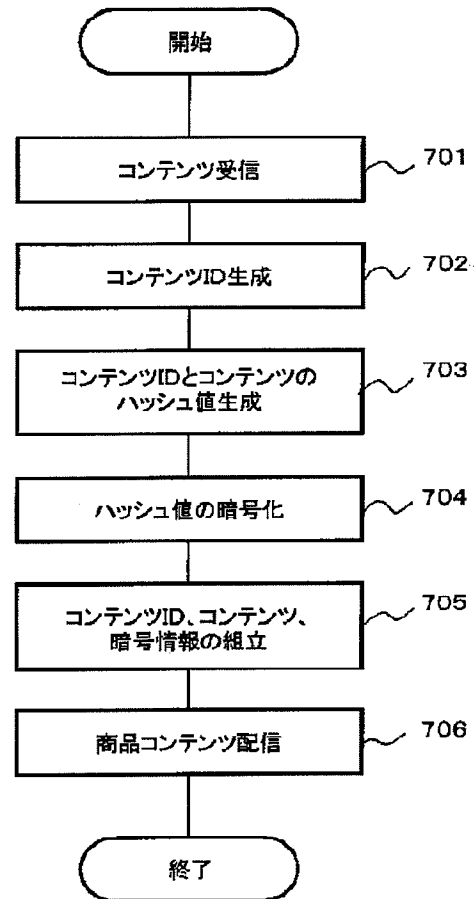
管理装置の構成図

【図7】



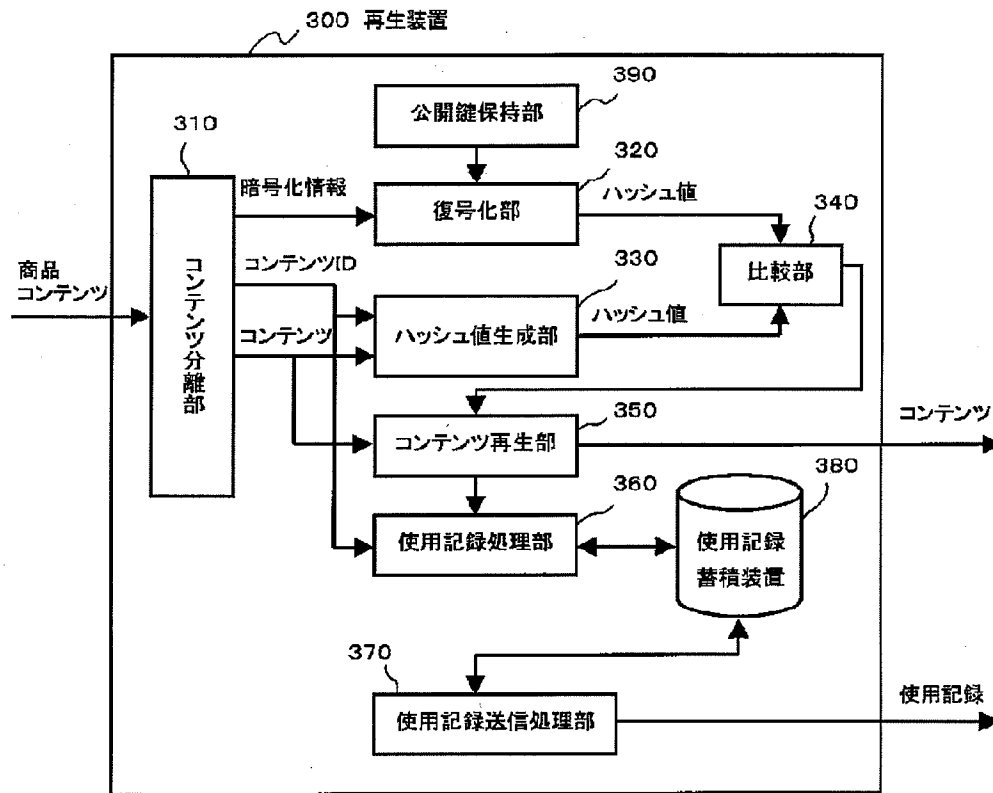
報酬分配時の処理フロー

【図9】



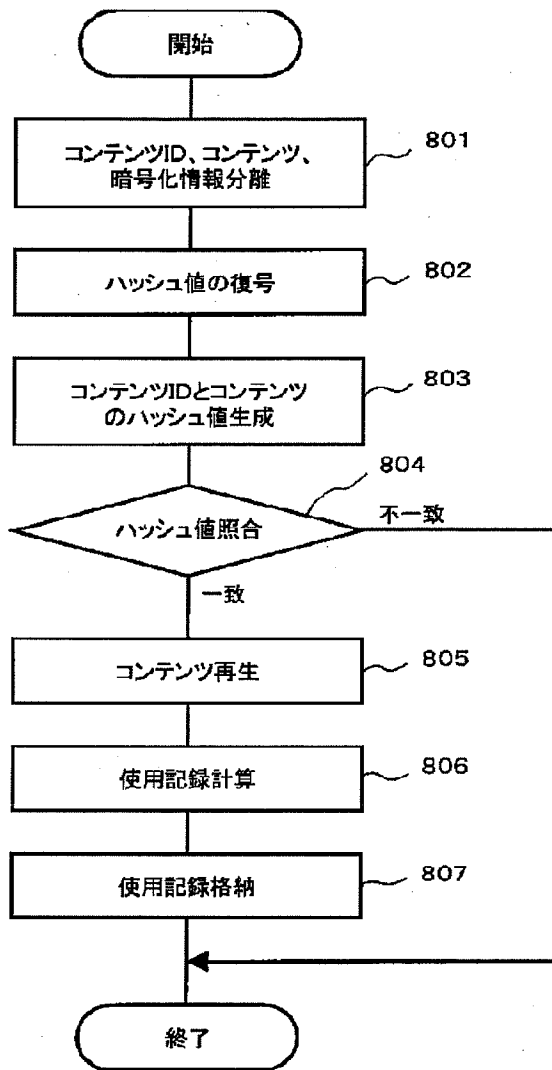
コンテンツ配信処理フロー図

【図10】



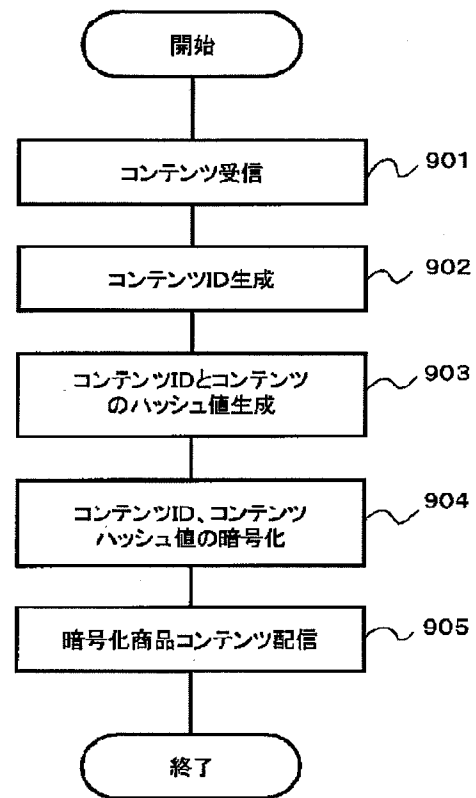
再生装置の構成図

【図11】



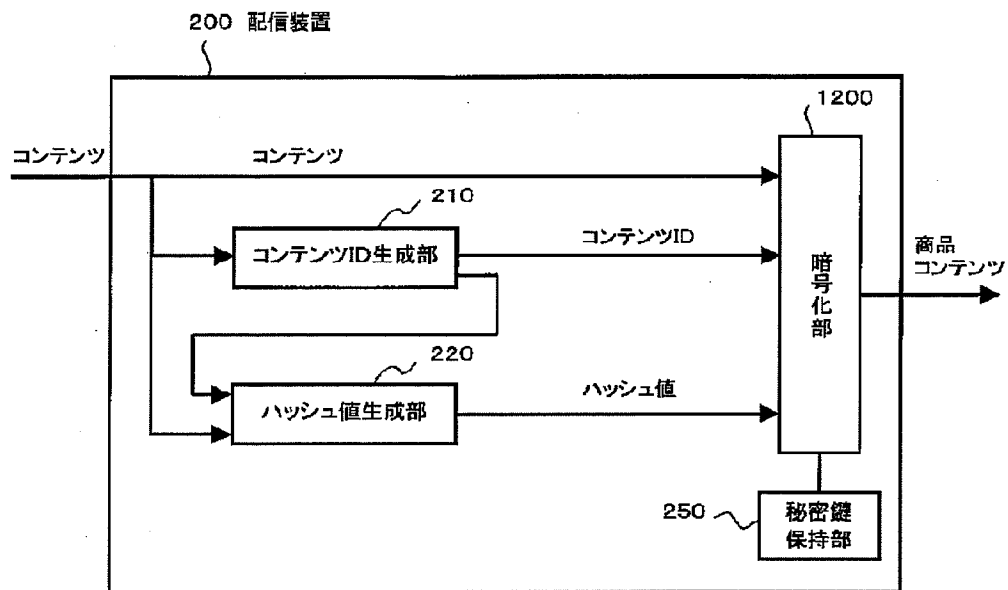
再生時の処理フロー

【図13】



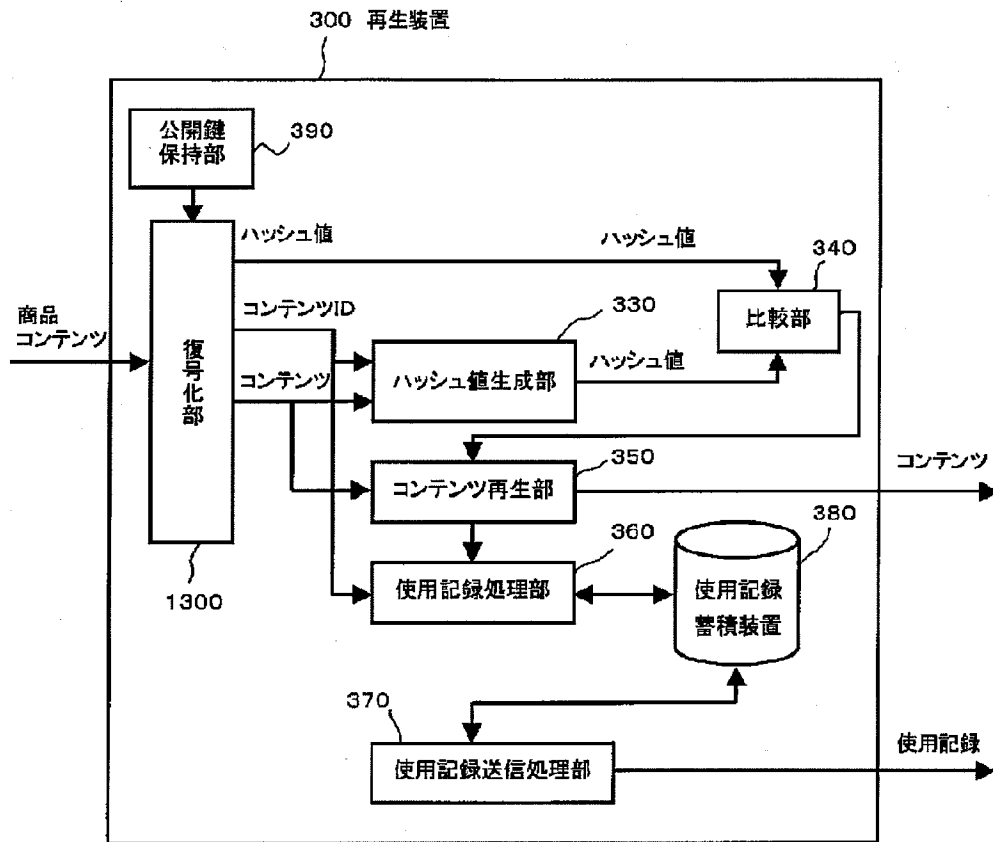
コンテンツ配信処理フロー図

【図12】



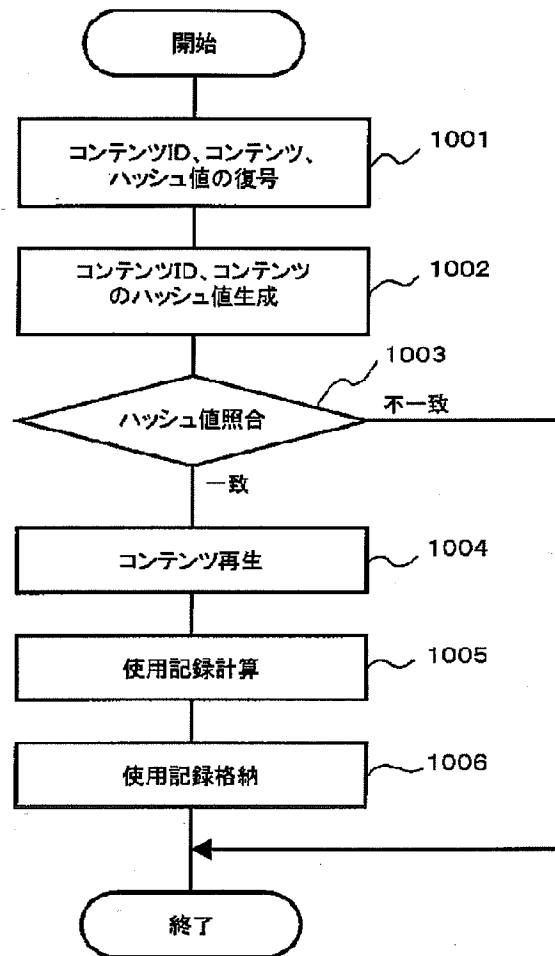
配信装置の構成図

【図14】



再生装置の構成図

【図15】



再生時の処理フロー

フロントページの続き

F ターム(参考) 5B017 AA02 BA07 CA16
5J104 AA07 AA08 LA03 LA05 PA07
PA10